Amendments to the Claims:

Current listing of the claims is herein provided. This listing will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method of securely transmitting sensitive data ~~using encryption~~ between a sender and a receiver, the method comprising:

generating a first encryption key on a sender First Information Processing System (FISP), the sender FIPS being under control of the sender and said first encryption key being unknown to a receiver FIPS being under control of the receiver;

encrypting on the sender FIPS said sensitive data ~~to be transmitted from the sender to the receiver~~ using said first encryption key, therefore generating encrypted sensitive data;

providing, separate from the sender FIPS and the receiver FIPS,~~separate~~ Second Information Processing Systems (SIPSs) ~~in secure local communication with both the sender and the receiver~~,a sender SIPS in secure local communication with the sender FIPS, and a receiver SIPS in secure local communication with the sender FIPS;

the sender FIPS transmitting to ~~its~~ the sender SIPS ~~the~~ said first encryption key and information relative to ~~dependent on an~~ identity of the receiver;

the sender SIPS ~~of the sender~~ selecting one of a plurality of second encryption keys, said selected second encryption key corresponding to the information transmitted by the sender FIPS ~~dependent on~~ regarding the identity of the receiver, and a unique second key identifier corresponding to said selected encryption second key, wherein said selected second key identifier and said ~~corresponding~~ selected second encryption key are known by the receiver SIPS while unknown by the receiver FIPS ~~being known to the SIPS of the receiver~~;

the sender SIPS ~~of the sender~~ encrypting the first encryption key using the selected second encryption key ~~to provide~~ therefore generating an encrypted first key;

the sender SIPS ~~of the sender~~ encrypting said second key identifier ~~corresponding to said selected second key~~ using a third encryption key known by the receiver SIPS while unknown by the receiver FIPS, ~~allowing the sender to retrieve~~

~~said identifier to provide an encrypted identifier to provide~~ therefore generating an encrypted second key identifier;

the sender SIPS communicating to the sender FIPS said encrypted first key and said encrypted second key identifier;

the sender FIPS combining said encrypted sensitive data, said encrypted first key, and said encrypted second key identifier into a message;

the sender FIPS transmitting said message ~~said encrypted first key, said encrypted second key identifier and said data to be transmitted from the sender~~ to the receiver FIPS ~~using said first key~~ over a generally unsecured transmission link;

the receiver FIPS extracting from said message said encrypted second key identifier and said encrypted first key;

the receiver FIPS communicating said encrypted second key identifier and said encrypted first key to the receiver SIPS;

~~transmitting from the receiver to the SIPS of the receiver said encrypted first key and said encrypted identifier;~~

the receiver SIPS ~~of the receiver~~ decrypting said encrypted second key identifier using the third encryption key ~~to retrieve from the SIPS device of the receiver the second encryption key~~;

the receiver SIPS retrieving said second encryption key using said second key identifier;

the receiver SIPS ~~of the receiver~~ decrypting said encrypted first encryption key using said second encryption key ~~to provide the receiver with the first encryption key~~;

the receiver SIPS communicating said first encryption key to the receiver FIPS; and

the receiver FIPS decrypting said sensitive data using said ~~the retrieved~~ decrypted first encryption key therefore generating decrypted sensitive data in a usable format for the receiver,

wherein the sender and the receiver are adapted to initiate a pairing process over said generally unsecured transmission link during which pairing process the sender SIPS and the receiver SIPS exchange signals to establish the use of a common second encryption key without communicating said second encryption key over said generally unsecured transmission link.

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Cancelled)

6. (Cancelled)

7. (Cancelled)

8. (Cancelled)

9. (Cancelled)

10. (Cancelled)

11. (Cancelled)

12. (Cancelled)

13. (Cancelled)

14 to 35. (Withdrawn)

36. (Currently amended) An information processing method comprising:

-generating a first key in a First Information Processing System (FIPS);

-encrypting sensitive data using the generated first key, thereby generating temporary secured sensitive data;

-selecting a correspondent to whom the sensitive data is destined;

-transmitting the first key and correspondent selection data from the FIPS to a Second Information Process System (SIPS) which is arranged separate from the FIPS;

-identifying among SIPS stored key identifiers and keys a correspondent key identifier and a correspondent key based on received correspondent selection data

from the FIPS;

-encrypting the first key using the identified correspondent key, thereby generating a secured first key in said SIPS;

-encrypting the identified correspondent key identifier using a SIPS stored public key, thereby generating a secured key identifier in said SIPS;

-transmitting the secured first key and the secured key identifier from the SIPS to the FIPS; and

-integrating into integrated secured sensitive data the temporarily secured data, the secured first key, and the key identifier,

wherein said correspondent key is established with a system operated by the correspondent prior to performing said information processing method without having communicated said identified correspondent key outside said SIPS.

37. (Original) The method of claim 36, further comprising authenticating a user and granting SIPS use to the user.

38. (Original) The method of claim 36, further comprising at least one of:

-storing integrated secured data on accessible holding means; and

-communicating integrated secured data to a correspondent FIPS.

39. (Original) The method of claim 36, further comprising erasing the first key, the temporarily secured sensitive data, and the SIPS communicated secured key and secured key identifier from the FIPS.

40. (Original) The method of claim 36, further comprising puzzling communication between the SIPS and the FIPS by at least one of:

-creating unnecessary signals between valuable signals transmitted to the FIPS; and

-modifying SIPS generated signals and data transmitted to the FIPS in order to render more difficult the reading of said signals and data.

41. (Currently amended) An information processing method comprising:

-extracting from integrated secured sensitive data a secured first key and a secured key identifier on a First Information Processing System (FIPS);

-transmitting the secured first key and the secured key identifier from the FIPS to a Second Information Processing System (SIPS) separate from the FIPS;

-decrypting the key identifier using a SIPS stored public key on the SIPS, thereby extracting a correspondent key identifier;

-identifying a correspondent key associated to the identified correspondent key identifier among SIPS stored keys and key identifiers on the SIPS;

-decrypting the secured first key using the identified correspondent key on the SIPS, thereby extracting a first key;

-transmitting the first key from the SIPS to the FIPS; and

-decrypting the sensitive data using the first key on the FIPS, thereby extracting sensitive data

wherein said correspondent key is established with a system which has generated said integrated secured sensitive data prior to performing said information processing method without having communicated said identified correspondent key outside said SIPS.

42. (Original) The method of claim 41, further comprising authenticating a user and granting SIPS use to the user.

43. (Original) The method of claim 41, further comprising storing extracted sensitive data on FIPS storing means.

44. (Original) The method of claim 41, further comprising erasing FIPS extracted data from the FIPS.

45. (Original) An information processing method comprising:

-receiving from an external information processing system a first key used to encrypt sensitive data and correspondent data designating to whom the sensitive data is destined;

-identifying a correspondent key and a correspondent key identifier among stored keys and key identifiers using the received correspondent data;

-encrypting the received key using the identified correspondent key, thereby generating a secured first key;

-encrypting the identified correspondent key identifier using a stored public key, thereby generating a secured key identifier; and

-transmitting the secured first key and secured key identifier to the external information processing system for integration into integrated secured sensitive data.

46. (Original) The method of claim 45, further comprising authenticating a user and granting a method processing authorization to the user.

47. (Original) The method of claim 45, further comprising puzzling communication between the SIPS and the FIPS by at least one of:

-creating unnecessary signals between valuable signals transmitted to the FIPS; and

-modifying SIPS generated signals and data transmitted to the FIPS in order to render more difficult the reading of said signals and data.

48. (Cancelled)

49. (Cancelled)

50 to 57. (Withdrawn)